

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月15日

出 願 番 号

Application Number:

特願2002-205072

[ST.10/C]:

[JP2002-205072]

出 願 人

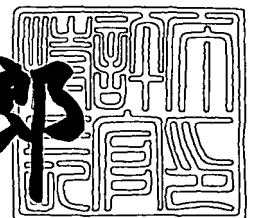
Applicant(s):

株式会社日立製作所

2003年 5月13日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3035564

【書類名】 特許願

【整理番号】 K02005601

【提出日】 平成14年 7月15日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00 330

【発明者】

【住所又は居所】 神奈川県海老名市下今泉 8 1 0 番地 株式会社日立製作所 インターネットプラットフォーム事業部内

【氏名】 幕田 好久

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100080001

【弁理士】

【氏名又は名称】 筒井 大和

【電話番号】 03-3366-0787

【手数料の表示】

【予納台帳番号】 006909

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報ネットワークシステムの制御方法および情報ネットワークシステムならびに移動通信端末

【特許請求の範囲】

【請求項 1】 有線または無線の情報ネットワークに複数の情報処理装置を接続した構成の情報ネットワークシステムの制御方法であって、

個々の前記情報処理装置の前記情報ネットワークに対する接続位置に関する第 1 位置情報と、当該情報処理装置の現在位置を示す第 2 位置情報とを用いて、当該情報処理装置の前記情報ネットワーク上における情報資源へのアクセスの可否を制御することを特徴とする情報ネットワークシステムの制御方法。

【請求項 2】 有線または無線の情報ネットワークと、前記情報ネットワークに接続され、当該情報ネットワーク上の情報資源にアクセスする第 1 情報処理装置と、前記第 1 情報処理装置の前記情報ネットワークに対する接続位置に関する第 1 位置情報および当該第 1 情報処理装置の現在位置を示す第 2 位置情報を用いて、前記第 1 情報処理装置の前記情報資源へのアクセスの可否を制御する第 2 情報処理装置と、を含むことを特徴とする情報ネットワークシステム。

【請求項 3】 有線または無線の情報ネットワークに接続される移動通信端末であって、前記情報ネットワークに接続するための第 1 通信手段と、当該移動通信端末の現在位置の取得に用いることが可能な第 2 通信手段と、前記現在位置情報を前記情報ネットワークに送出する機能とを含むことを特徴とする移動通信端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報ネットワーク技術および移動通信端末に関し、特に、共有可能なファイル等の情報資源を持つ複数の端末とファイルサーバが有線または無線でネットワーク接続された環境において、認証サーバがおのこの端末とファイルサーバの位置情報を元にファイルの共有制御をする認証技術に関する。

【0002】

【従来の技術】

端末やファイルサーバは、情報の共有を実現するためにネットワークを通じて接続されている。無線ネットワーク接続においては、端末やファイルサーバは無線 LAN のアクセスポイントを通じて無線電波で通信を確立できる。

【0003】

しかし、その無線電波の到達範囲は不定であり、無線電波到達範囲内に存在する想定外の端末がネットワークに接続し、悪意ある使用者がその端末を操作して証拠を残さずに、別な端末やファイルサーバから情報を入手できる可能性がある。

【0004】

【発明が解決しようとする課題】

上記従来技術では、無線通信の可能な範囲が限定されないため、無線電波到達範囲内に存在する想定外の端末がネットワークに接続された場合について配慮がされておらず、情報漏洩を引き起こす懸念がある、という技術的課題があった。

【0005】

なお、特開 2000-215169 号公報には、無線端末の LAN へのアクセスポイント毎に特定データセットを割り当てることにより、アクセスポイントが変化する毎に当該特定データセットへのアクセスが自動的に行われるようにした技術が開示されているが、当該無線端末の位置を識別するために用いられる位置情報はアクセスポイントの位置情報のみであるため、たとえば建物内の各部屋毎にアクセスポイントを割り当てて各部屋を移動する毎にアクセス可能なデータセットを切り替えることはできるものの、建物の外からのアクセスが識別できず、情報漏洩等の上述の技術的課題は依然として解決されない。

【0006】

本発明は、通信の可能な範囲を限定し、想定外の端末からのネットワーク接続を拒否することを目的としており、限定された範囲内でのみのネットワーク接続環境を提供し、情報漏洩やなりすましを防ぎ的確な情報伝達を可能とすることを目的とする。

【0007】

また、本発明は、各端末およびファイルサーバにおいて、自身と複数のGPS衛星または複数の携帯電話基地局との間の距離から、自身の位置情報を取得することを目的とする。

【0008】

さらに、本発明は、認証サーバにおいて、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうことを目的とする。

【0009】

【課題を解決するための手段】

本発明は、有線または無線の情報ネットワークに複数の情報処理装置を接続した構成の情報ネットワークシステムの制御方法であって、個々の情報処理装置の情報ネットワークに対する接続位置に関する第1位置情報と、当該情報処理装置の現在位置を示す第2位置情報とを用いて、当該情報処理装置の情報ネットワーク上における情報資源へのアクセスの可否を制御するものである。

【0010】

より具体的には、一例として、有線、あるいは無線でネットワーク接続された端末やファイルサーバの現在位置情報（第2位置情報）を取得し、認証サーバにおいてそれぞれの現在位置情報と、アクセスポイント（ネットワークセグメント）の位置情報（第1位置情報）に基づいて、それぞれの通信可能範囲の設定を行ない、それぞれが限定された範囲内にある端末やファイルサーバとのみ情報の送受信を行なう。

【0011】

また、上記構成において、端末やファイルサーバの位置情報は、それ自身と複数台のGPS衛星との距離から得た情報を元に取得する。もしくは、端末やファイルサーバの位置情報は、それ自身と複数台の携帯電話基地局との距離から得た情報を元に取得する。もしくは、端末やファイルサーバの位置情報は、それ自身とその端末やファイルサーバが接続可能な無線LANアクセスポイントの位置情報を元に取得する。

【0012】

そして、上記構成において、認証サーバは、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なう。

【 0 0 1 3 】

端末またはファイルサーバは、認証サーバ経由で他の端末またはファイルサーバからファイルを取り出すことができる。

【 0 0 1 4 】

ある端末に対するアクセス要求がその端末の通信可能範囲から逸脱していた場合、認証サーバはその端末に対するアクセスを認めないことでアクセス制御を行なう。

【 0 0 1 5 】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【 0 0 1 6 】

図 1 は、本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の一例を示す概念図である。

【 0 0 1 7 】

本実施の形態では、情報ネットワークの一例として、各端末がそれぞれに GPS (Global Positioning System) 等によって位置情報を得て、認証サーバにおいて共有する端末決定するネットワークシステムを例に採って説明を進める。

【 0 0 1 8 】

本実施の形態のネットワークシステムは、図 1 に示すように、共有可能なファイルを持つ自由に移動可能な複数の端末 3 0 0, 3 0 1, 3 1 1 ~ 3 1 5 (以下、端末 3 x x と総称する) と、共有可能なファイルを持つ特定位置に固定されたファイルサーバ 4 1 1 ~ 4 1 3 (以下、4 1 x と総称する) と、端末 3 x x の位置情報を収集し各端末のアクセス許可範囲を決定しアクセス制御を行なう認証サーバ 4 0 0 と、各端末 3 x x が認証サーバ 4 0 0 に接続するために設置する無線 LAN アクセスポイント 1 0 1 と、端末 3 x x の位置情報を得るのに使用する複数の GPS 衛星 5 0 1, 5 0 2, 5 0 3 (以下、5 0 x と総称する) と、から成

る。

【0019】

端末 3 x x の各々は、無線 LAN アクセスポイントとの間における無線通信を行うための無線 LAN アクセス機能 300 a と、GPS 衛星 50 x との通信にて当該端末 3 x x の現在位置情報を得る GPS 受信機能 300 b と、この現在位置情報を無線 LAN 上に送出する機能とを備えている。

【0020】

また、ファイルサーバ 41 x の各々も自身の位置情報を取得して認証サーバ 400 に送出する機能を備えることができる。

【0021】

なお、端末 3 x x が携帯電話機能を含む場合には、GPS 受信機能 300 b としては、公衆携帯電話網の図示しない基地局との位置関係から現在位置を取得する機能が実装される。

【0022】

図 2 は、共有可能なファイルを持つ端末、ファイルサーバがどの領域にある端末に対してアクセスを認めるか否かを制御する認証処理に用いられる情報テーブルの構成の一例を示す概念図である。

【0023】

本実施の形態の情報テーブル 600 は、無線 LAN アクセスポイント 600 a の各々毎に、アクセス許可領域 600 b、許可範囲 (x, y) 座標からなる受信許可範囲 600 c、アクセス先端末リスト 600 d、アクセス元端末リスト 600 e の各情報に対応付けて格納されている。なお、無線 LAN アクセスポイント 600 a、アクセス許可領域 600 b、アクセス先端末リスト 600 d、アクセス元端末リスト 600 e の各数値は、図 1 の各部の符号を示している。

【0024】

また、受信許可範囲 600 c の許可範囲 (x, y) 座標の数値は、簡単のため簡略な数値が設定されているが、実際には、たとえば、各端末の現在位置（経度，緯度等）に基づく認証の基準値が設定されている。

【0025】

共有可能なファイルを持つファイルサーバ 4 1 1 は、アクセス許可領域として領域 2 1 1 が設定されていて、情報テーブル 6 0 0 に保存されている。

【 0 0 2 6 】

領域 2 1 1 内にある端末 3 1 1 は、無線 LAN アクセスポイント 1 0 1 と通信が可能であり、かつ GPS 衛星 5 0 x から情報の取得が可能である。

【 0 0 2 7 】

端末 3 1 1 は、GPS 衛星 5 0 x より情報を取得し、その情報を元に自身の位置情報を算出する。

【 0 0 2 8 】

端末 3 1 1 は、自身の位置情報を無線 LAN アクセスポイント 1 0 1 を経由して認証サーバ 4 0 0 に送信する。

【 0 0 2 9 】

また端末 3 1 1 は、認証サーバ 4 0 0 から自身の位置情報の送信要求があった場合、速やかに自身の現在の位置情報を返信する。

【 0 0 3 0 】

なお、この端末からの現在位置情報の送信方法としては、標準の無線 LAN プロトコルの接続開始時等の情報フレームにおけるベンダユニークな領域を使用することが考えられる。そして、認証サーバでは、当該ベンダユニークな領域に所定のフォーマットにて位置情報が設定されている場合には、送信元の当該端末が本実施の形態の認証技術に対応した機能を持つものとして、ファイルサーバへのアクセス許可等の後述の認証処理を実行し、設定されていない場合には、一般の端末として、最もセキュリティレベルの低い一般公開用データのみにアクセスさせる等の処理を行うことができる。

【 0 0 3 1 】

これにより、既存の無線 LAN プロトコルの汎用性を損なうことなく、本実施の形態の認証機能を実装することができる。

【 0 0 3 2 】

このような端末 3 x x の動作の一例を図 7 のフローチャートに例示する。

【 0 0 3 3 】

すなわち、まず、GPS等から自身の現在位置情報を取得する動作（ステップ921）を、最寄りの無線LANアクセスポイントの通信可能領域に入るまで繰り返し（ステップ922）、通信可能領域に入ったら、認証サーバ400に現在位置情報および接続中の無線LANアクセスポイント（ネットワークセグメント）の位置情報を、無線LANアクセスポイントを経由して送信してアクセス要求を行う（ステップ923）。

【0034】

そして、認証サーバ400からのアクセス許可信号を待ち（ステップ924）、アクセス許可の場合には（ステップ925）、ファイルサーバへのアクセス要求を行い（ステップ926）、データを取得する（ステップ927）。また、アクセス不許可の場合には、ファイルサーバへのアクセスを行わない（ステップ928）。

【0035】

認証サーバ400は、受信した端末311の位置情報が、図2の情報テーブル600のアクセス許可範囲内に収まっている場合、アクセス元端末リスト600eに端末311を加える。

【0036】

また、アクセス元端末リスト600eに登録された端末に対して、その端末の位置情報を定間隔で要求し、受信した端末の位置情報が情報テーブル600のアクセス許可範囲から外れた場合や、位置情報の返信が無い場合は、アクセス元端末リスト600eから端末情報を削除する。

【0037】

ここで、端末311がファイルサーバから情報を取得しようとするとき、自身がいる領域211がアクセスを許可している端末について認証サーバ400に問い合わせをする。

【0038】

認証サーバ400は、情報テーブル600を参照し、領域211に対応する行601が指し示すアクセス元端末リスト600eに端末311の情報があるので、端末311に対して、領域211に対応するアクセス先端末リスト600dに

登録されているファイルサーバ411に対するアクセスを許可する。

【0039】

情報テーブル600を参照した結果、領域211に対応する行601が指し示すアクセス元端末に端末311の情報が無ければ、端末311はすでに領域211外に出たものとみなし、アクセスを認めない。

【0040】

これにより、端末311は領域211にいる限り、無線LANアクセスポイント101、ネットワークを経由してファイルサーバ411から情報を取得できる。

【0041】

他の端末についても同様である。

【0042】

領域212内にある端末312は、ファイルサーバ412にアクセス可能である。

【0043】

領域213内にある端末313、314は、ファイルサーバ413と端末300にアクセス可能である。

【0044】

また、別な無線LANアクセスポイント102からネットワーク接続している、領域214内の端末315は、端末312と端末301にアクセス可能であるが、端末301がネットワークに接続されていないので、端末312にのみアクセス可能である。

【0045】

領域200にある端末301は、どの無線LANアクセスポイントとも通信が可能でないため、認証サーバ400に接続することができない。無線LANアクセスポイント101または102の通信可能範囲に入ると初めて認証サーバへの接続に成功し、領域のアクセス設定に従い通信が可能となる。

【0046】

上述のような認証サーバの動作の一例を図6のフローチャートを参照して説明

する。

【0047】

任意の端末3xxが任意の無線LANアクセスポイントの通信可能範囲内にあるかを監視し（ステップ911）、通信可能範囲内にある場合には、当該端末から当該端末の現在位置情報を取得し（ステップ912）、当該端末の現在位置が個々の無線LANアクセスポイント毎に設定された受信許可範囲内にあるかを調べ（ステップ913）、受信許可範囲内にある場合には、当該端末にアクセス許可信号を送信し（ステップ914）、情報テーブル600のアクセス元端末リストに追加する（ステップ915）。

【0048】

ステップ913で範囲外の場合には、当該端末にアクセス不許可を通知し（ステップ916）、アクセス元端末リストから当該端末を削除する（ステップ917）。

【0049】

同様に、図5にて、ファイルサーバの動作の一例を説明する。

【0050】

任意の端末からのアクセス要求を監視し（ステップ901）、要求がない場合には当該端末との送受信を停止する（ステップ902）。

【0051】

アクセス要求がある場合には自ファイルサーバのマルチメディア情報等の情報配信サービス等に対応した端末か否かを判別し（ステップ903）、未対応の場合にはサービス案内を通知する（ステップ904）。

【0052】

サービス対応の端末の場合には、さらに、アクセス元端末リストに当該端末が登録されているか調べ（ステップ905）、登録済み（すなわち、認証済み）の場合には、当該端末との送受信を確立する（ステップ907）。未登録の場合には、当該端末にアクセス不可メッセージを送信する（ステップ906）。

【0053】

ところで、もし、無線LANアクセスポイント101と102が同じビル内の

異なる階をカバーする領域を持つ場合、GPS衛星から得た位置情報のみではその端末がどの階にあるのか、認証サーバ400は把握できない。この技術的課題の解消のために、本実施の形態では、その端末が使用している無線LANアクセスポイント（ネットワークセグメント）も記録しておき、端末の現在位置と併用して認証に用いることで、高さ方向の違いも考慮可能である。これは、無線LANで使用する電波がビルの壁を通り抜けないことを利用している。

【0054】

すなわち、図3に例示されるように、二階建ての建物700の一階フロア211a（1F）、二階フロア214a（2F）の各々に無線LANアクセスポイント101、102を設置し、無線LANアクセスポイント101に対する端末のアクセス許可領域として領域211を一階フロア211aの床範囲に設定し、同様に無線LANアクセスポイント102に対する端末のアクセス許可領域として領域214を二階フロア214aの床範囲に設定しておく。そして、認証サーバ400では、個々の端末311、315の現在位置情報の他に無線LANアクセスポイント101、102の位置情報を、ファイルサーバ41x等の持つデータへのアクセスの可否を決定する認証に用いることで、各階毎に当該階内に位置する個々の端末311、315を正確に識別でき、的確なデータアクセス制御が可能になる。

【0055】

この方法による利点は、無線LANアクセスポイント101、102の通信可能領域201、202の範囲内であっても、特定範囲の外にある端末とファイルの共有をするための通信を遮断することができ、また端末側にこのシステムに対する特殊な機構を用意する必要が無い。不正な端末を排除する目的での使用を想定できる。

【0056】

すなわち、たとえ、建物700からの無線LANの電波漏洩があっても、建物700の外部に位置する端末が無線LANに接続できたとしても、その端末の現在位置情報がアクセス許可領域の外であると判定できるため、認証不可と判定することができ、データアクセスのセキュリティを維持できる。

【 0 0 5 7 】

上述の本実施の形態の認証方法を応用することで、例えば図 4 のような CD ショップの運営に適用できる。

【 0 0 5 8 】

CD ショップ 8 0 0 内は各ジャンルごとに領域が決められていて、領域 2 1 はロックの CD が陳列してある場所、領域 2 2 はジャズ CD が陳列してある場所とする。それぞれの領域に対応した試聴用の音楽ファイルがファイルサーバ 4 1 に格納されている。また、認証サーバ 4 0 により、領域 2 1 および領域 2 2 は、それぞれロック音楽、ジャズ音楽の試聴データに対応付けられている。

【 0 0 5 9 】

CD ショップを通信可能範囲 2 0 内に含む無線 LAN アクセスポイント 1 に対する無線 LAN アクセス機能 3 a と GPS 衛星 5 0 x からの GPS 受信機能 3 b を備えた携帯電話 3 を持った客が CD ショップ内を歩いていて、領域 2 1 内で携帯電話 3 を操作して試聴をしようとする、認証サーバ 4 0 が携帯電話 3 の現在位置情報に基づいてロック音楽の試聴データを当該携帯電話 3 に送信することでロック音楽の試聴データが携帯電話 3 の画面に表示され、そのデータを試聴できる。

【 0 0 6 0 】

同様にして、領域 2 1 を外れ領域 2 2 に移動すると、ロック音楽の試聴はできなくなり、代わりにジャズ音楽の試聴ができるようになる。

【 0 0 6 1 】

また、領域 2 1 および領域 2 2 が同一建物内の別階フロアの場合には、無線 LAN アクセスポイントの位置情報を併用することで同様の切り替えや認証が可能なことは上述のとおりである。

【 0 0 6 2 】

この方法により、特定範囲に位置する携帯電話 3 にだけ試聴データを提供し、また以降の試聴データの不正使用も防ぐことができる。

【 0 0 6 3 】

他にも、オフィスにおいて外部に社内の情報が漏れないようにする手段など、

さまざまな応用方法が考えられる。

【 0 0 6 4 】

以上説明したように、本実施の形態によれば、共有可能なファイルを持つ複数の端末 3 x x やファイルサーバ 4 1 x が、有線または無線でネットワーク接続された環境において、認証サーバ 4 0 0 が各々の端末とファイルサーバ 4 1 x の位置情報を元にファイルの共有制御をするので、ネットワーク上のファイルに対するアクセス制御が可能となり、不正アクセスや成りすましの防止に効果がある。

【 0 0 6 5 】

さらに各端末 3 x x およびファイルサーバ 4 1 x において、自身と複数の G P S 衛星 5 0 x または複数の携帯電話基地局との間の距離から、自身の位置情報を取得するが、端末 3 x x とファイルサーバ 4 1 x に G P S 受信装置もしくは、携帯電話受信装置を装着するのみで、すでに G P S 衛星や携帯電話基地局が整備されており、いま現在あるものより大きな投資をすることなく、不正アクセスや成りすましの防止を効果的に実現できる。

【 0 0 6 6 】

さらに、認証サーバ 4 0 0 において、各端末 3 x x およびファイルサーバ 4 1 x から受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうので、正しい位置情報に基づいたアクセスに対してのみ通信を許可できるので、不正アクセスや成りすましの防止に効果がある。

【 0 0 6 7 】

本願の特許請求の範囲に記載された発明を見方を変えて表現すれば以下の通りである。

【 0 0 6 8 】

(1) . 共有可能なファイルを持つ複数の端末とファイルサーバが有線または無線でネットワーク接続された環境において、認証サーバがおのこの端末とファイルサーバの位置情報を元にファイルの共有制御をすることを特徴とするファイルアクセスの認証方法。

【 0 0 6 9 】

(2) . 項目 (1) 記載の各端末およびファイルサーバにおいて、自身と複数

のGPS衛星または複数の携帯電話基地局との間の距離から、自身の位置情報を取得することを特徴とする方法。

【0070】

(3)、項目(1)記載の認証サーバにおいて、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうこと特徴とする方法。

【0071】

以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【0072】

【発明の効果】

通信の可能な範囲を限定し、想定外の端末からのネットワーク接続を的確に拒否して、限定された範囲内でのみのネットワーク接続環境を提供し、情報漏洩やなりすましを防ぎ的確な情報伝達を可能とすることができる、という効果が得られる。

【0073】

各端末およびファイルサーバにおいて、自身と複数のGPS衛星または複数の携帯電話基地局との間の距離から、自身の位置情報を取得してセキュリティ管理に適用することができる、という効果が得られる。

【0074】

認証サーバにおいて、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうことができる、という効果が得られる。

【図面の簡単な説明】

【図1】

本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の一例を示す概念図である。

【図2】

本発明の一実施の形態である情報ネットワークシステムの制御方法において用いられる情報テーブルの一例を示す概念図である。

【図 3】

本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の変形例を示す概念図である。

【図 4】

本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の応用例を示す概念図である。

【図 5】

本発明の一実施の形態である情報ネットワークシステムにおけるファイルサーバの動作の一例を説明するフローチャートである。

【図 6】

本発明の一実施の形態である情報ネットワークシステムにおける認証サーバの動作の一例を説明するフローチャートである。

【図 7】

本発明の一実施の形態である情報ネットワークシステムにおける端末の動作の一例を説明するフローチャートである。

【符号の説明】

- 1 0 1, 1 0 2 無線 LAN アクセスポイント
- 2 0 0 無線 LAN アクセスポイントとの通信ができない領域
- 2 0 1 無線 LAN アクセスポイント 1 0 1 と通信可能な領域
- 2 0 2 無線 LAN アクセスポイント 1 0 2 と通信可能な領域
- 2 1 1 ~ 2 1 4 アクセス許可領域
- 3 0 0, 3 0 1, 3 1 1 ~ 3 1 5 自由に移動可能な端末 (第 1 情報処理装置)
- 3 0 0 a 無線 LAN アクセス機能 (第 1 通信手段)
- 3 0 0 b GPS 受信機能 (第 2 通信手段)
- 4 0 0 認証サーバ (第 2 情報処理装置)
- 4 1 1 ~ 4 1 3 ファイルサーバ (特定の位置に固定された端末)
- 5 0 1 ~ 5 0 3 GPS 衛星

6 0 0 認証サーバが持つ情報テーブル

6 0 1 ~ 6 0 3 情報テーブルの各アクセス許可領域の行

1 無線 LAN アクセスポイント

2 0 無線 LAN アクセスポイントの通信可能範囲

2 1 ロック CD 売り場 (領域)

2 2 ジャズ CD 売り場 (領域)

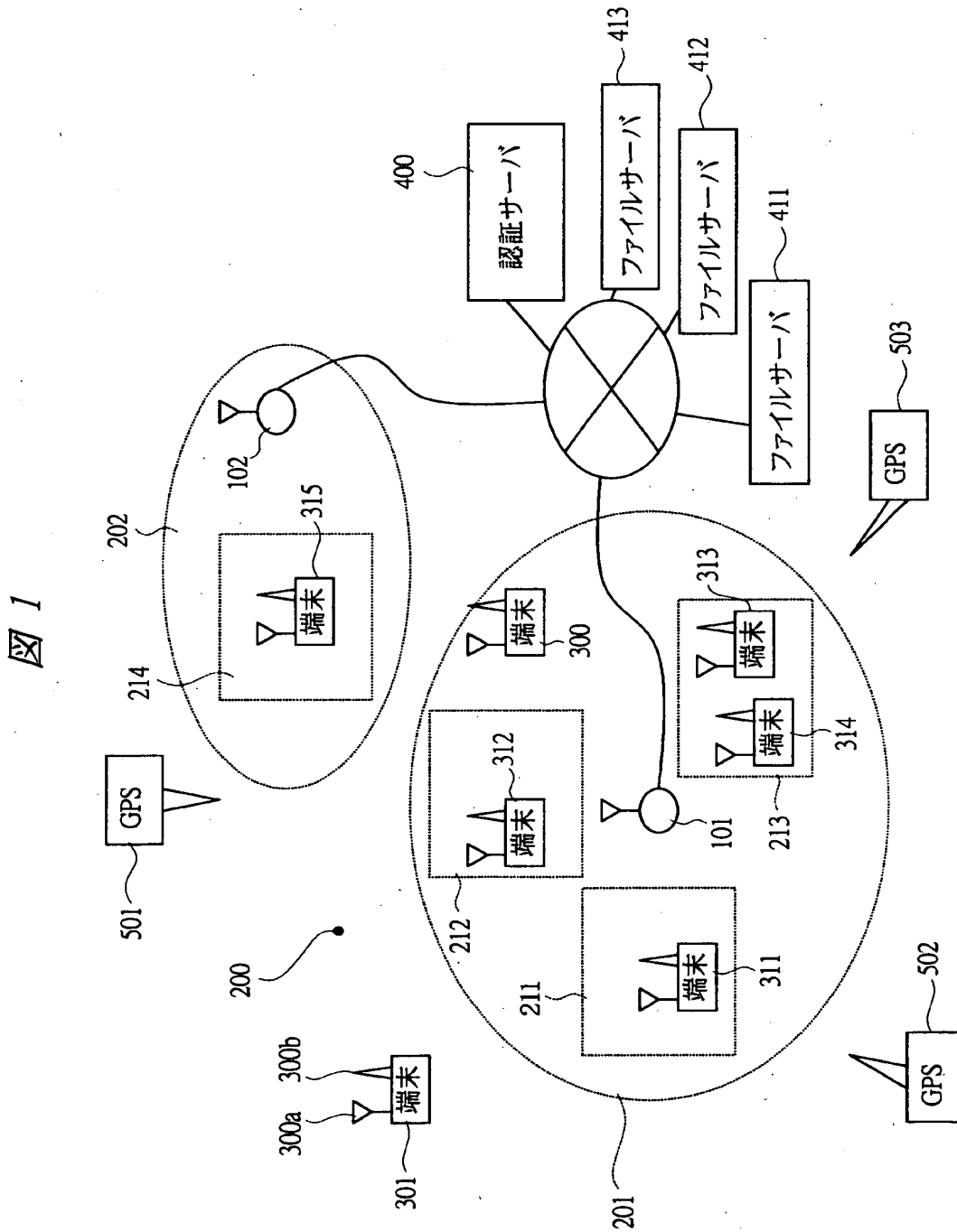
3 携帯電話

4 0 認証サーバ

4 1 ファイルサーバ

【書類名】 図面

【図 1】



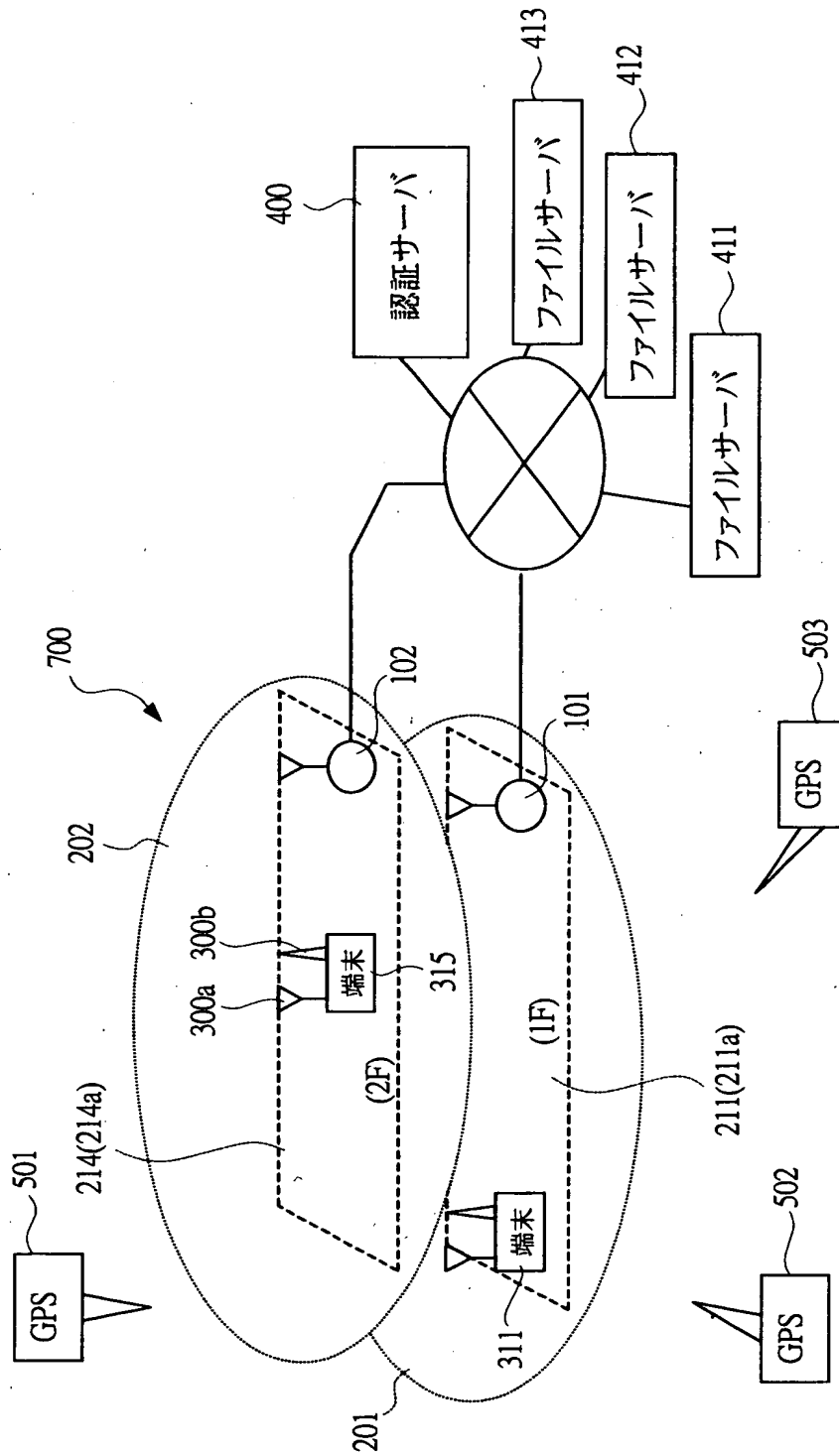
【図 2】

図 2

	無線 LAN AP	アクセス 許可領域	受信許可範囲		アクセス先 端末リスト	アクセス元 端末リスト
			X	Y		
601	101	211	10-12	32-34	411	311
602	101	212	12-14	30-32	412	312
603	101	213	13-15	33-35	413	313,314
	102	214	14-16	27-29	312,301	315

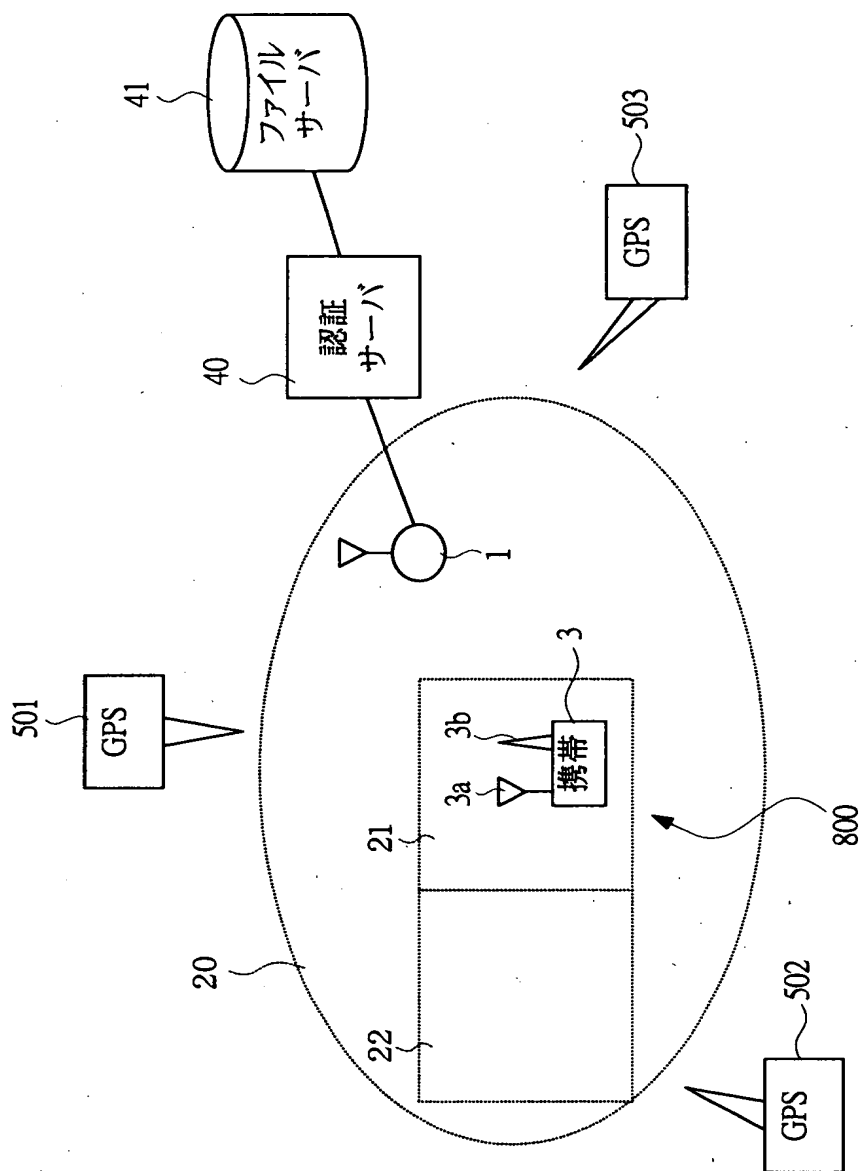
【図3】

図3



【図4】

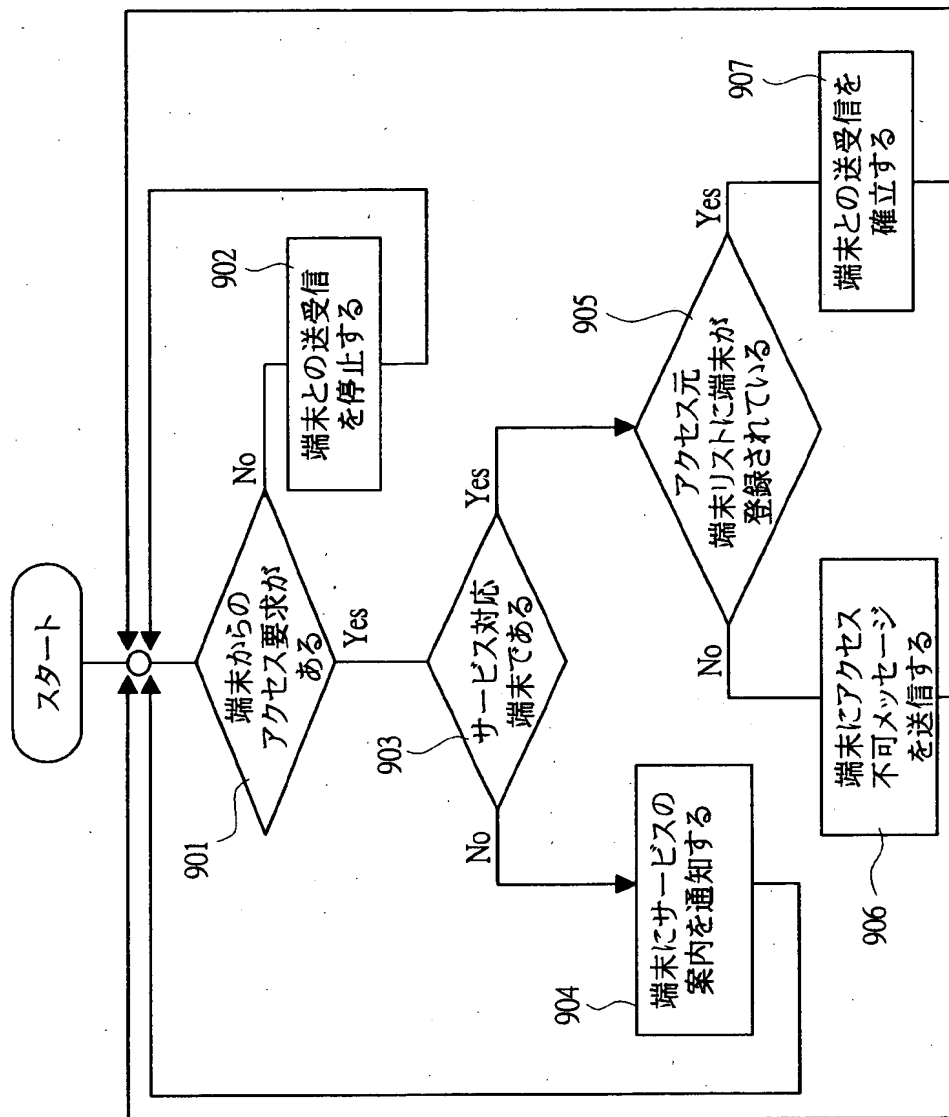
4



【図5】

図5

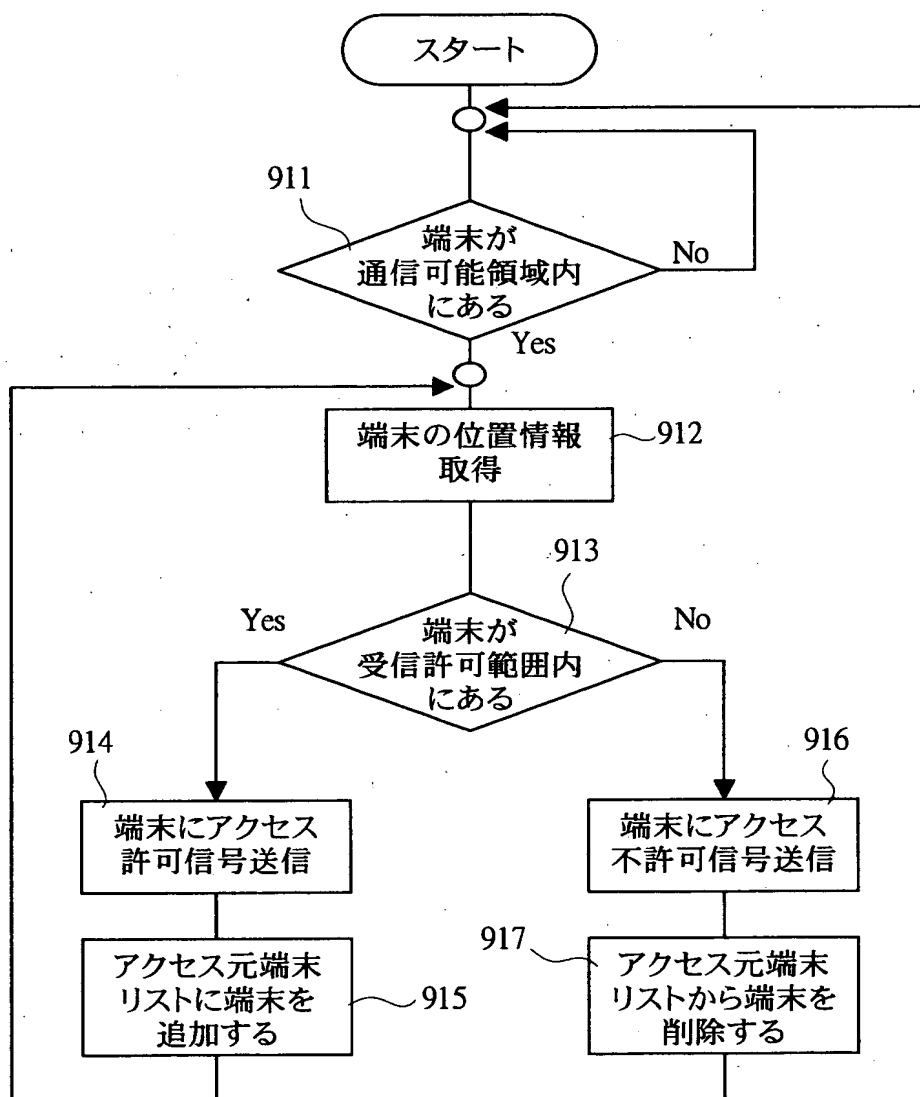
ファイルサーバのプロローチャート



【図6】

図6

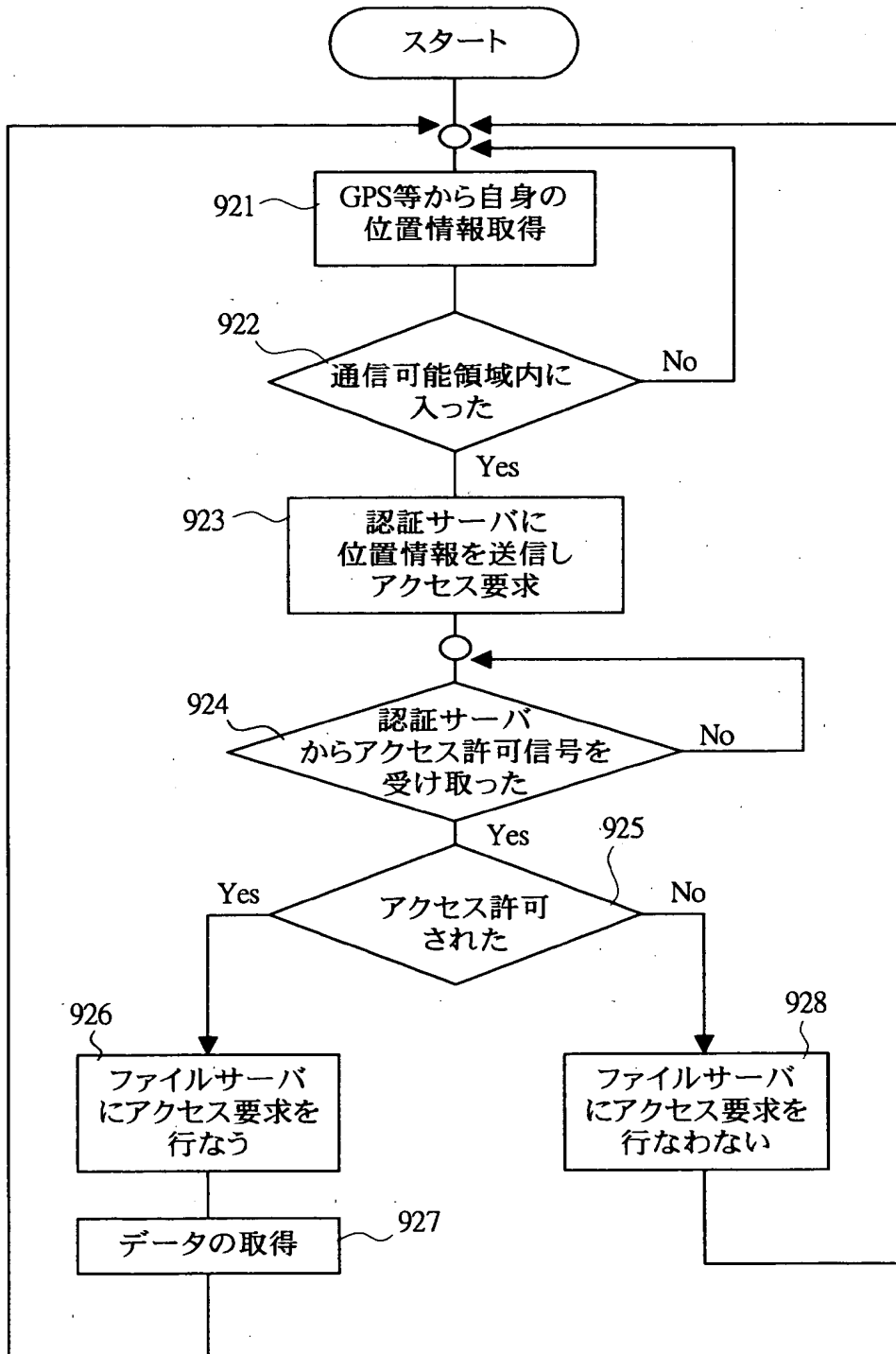
認証サーバのフローチャート



【図 7】

図 7

端末のフローチャート



【書類名】 要約書

【要約】

【課題】 無線ネットワーク上の情報資源に対するアクセス可能範囲を限定することで、不正アクセスの防止や的確な情報伝達を可能とする。

【解決手段】 端末 3 1 1 やファイルサーバ 4 1 1 ～ 4 1 3 は、複数の G P S 衛星 5 0 1 ～ 5 0 3 から受信した物理的な距離、複数の携帯電話基地局から受信した物理的な距離等の自身の現在位置情報と、無線 L A N ネットワークのセグメント（アクセスポイント）情報等の位置情報を認証サーバ 4 0 0 へ送信する。認証サーバ 4 0 0 はその位置情報の正当性を判断し、ネットワーク上のファイル等の情報資源へのアクセスを制御する。ネットワーク上のファイル装置に対するアクセス可能範囲を限定することで、自由に移動可能な端末に対して、不正アクセスの防止や的確な情報伝達が可能となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所